



## LSB Image Steganography with DES Cryptography

Nutan Manwade

Mtech Research Scholar,  
Sanghvi Institute of Management and  
Science, Indore, M.P., India

Swati Nigam

Assistant Professor,  
Sanghvi Institute of Management and  
Science Indore, M.P., India

**Abstract:** *In Steganography, the total message will be invisible into a cover media such as text, audio, video, and image in which attackers don't have any idea about the original message that the media contain and which algorithm use to embed or extract it. For better security DES cryptography technique has also been used in the proposed method. Before applying the Steganography technique, DES cryptography will change the secret message into cipher text to ensure two layer security of the message. In the proposed technique, a new Steganography technique is being developed to hide large data in image. This method is an improvement of Least Significant Bit (LSB) method for hiding information in images. It is being predicted that the proposed method will able to hide large data in a single image retaining the advantages and discarding the disadvantages of the traditional LSB method. Various sizes of data are stored inside the images and the PSNR are also calculated for each of the images tested. Based on the PSNR value, the Stego image has higher PSNR value as compared to other method. Hence the proposed Steganography technique is very efficient to hide the secret information inside an image.*

**Keywords:** *Image Steganography, DES Cryptography, Conceal of Message, LSB Image Steganography.*

### I. INTRODUCTION

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be more safe and secure[13]. In our daily life we use many insecure pathways for transferring and sharing information using internet or telephonically, but Sometimes it's not safe. Steganography and Cryptography there are two methods which could be used to sharing information in a encrypted manner. In process of cryptography includes modification of a message in which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn't be accessed. But in steganography the secret message is made to hide in cover image so that it could not be clear to any intermediate person that whether there is any message hidden in the information being shared, whereas in cryptography it's always clear to intermediate person that the message is in encrypted form. Secret message is covered by cover image and then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender[13].

- A. Data Security:** - In data security data has been changed. We implementing a new data security technique is called steganography, it means not only the meaning of data is change but also secure the presence of data from the other person. This system is hiding large amount of authenticated and encrypted data with respect of the size, dimensions of the image and without disturbing the clarity of the image.
- B. Cryptography:** - The word Cryptography is derived from the Greek words "cryptos" (meaning "hidden") and "graphy" (meaning "write"[3]). The study of Cryptography is meaning of converting information into an encrypted format, rendering it unreadable without the secret knowledge. The process of converting information (plain text) by transforming it into unreadable format (cipher text) is known as encryption[3]. The techniques of encryption can be sometimes broken by cryptanalysis, and then these is called as code breaking, although the modern techniques of cryptography are virtually unbreakable. Cryptography encrypts the plain text that is being sent. These mathematical schemes employ algorithms to actual data into unreadable data or text.
- C. Steganography:** - Steganography is an art and specially a science of hiding some information into another information. Steganography is an art because in ancient time steganography was used with some art like message written through invisible ink, Message engraved on the shaved head of slaves and then allow them to grow hair and at the receiver side receiver again shaved their head to read the secret message etc. Steganography is a science because in today's world we hide secret information i.e. text, audio, video etc. bit wise. Steganography is a technique of hiding secret messages inside a carrier so that only sender and intended recipient of the message know about the presence of hidden message. Steganography was derived from Greek words whose actual meaning is "hidden writing" (Greek word "Steganos" means "covered" and "graphy" means "writing")[4].

### II. COMPARISON BETWEEN STEGANOGRAPHY AND CRYPTOGRAPHY

With the increasing number of users and the number of unauthorized access has also increased. Hence, Information security plays an important role. Keeping this concept in mind cryptography and steganography both are used. Therefore,

the main issue now is to mitigate and to lessen the impact of the chances of the information being detected during transmission.

Cryptography deals message encryption but the communication is visible but on the other hand, steganography deals with secret message hiding but the communication is not visible. The major difference between steganography and cryptography is that encoding the traffic, the communications will be secured but people become aware of the existence of message by observing coded information, although they are not able to comprehend the data. In Steganography method hides the existence of the message so that intruders can not detect the communication and thus provides a higher level of security than cryptography. Both steganography and cryptography systems provide secret communications but different in terms of breaking the system. Steganography system is more easily breakable than cryptography systems in terms of system failure.

### **. III. BACKGROUND**

Besides cryptography, steganography can be employed to secure information in digital media. Cryptography and steganography techniques of digital images are widely used to prevent and frustrate opponent's attacks from unauthorised access.[3 ].There are many steganography techniques have been proposed:-

1. Spatial Domain technique
2. Transform Domain technique
3. Distortion technique
4. Masking and Filtering

1. **Spatial Domain Methods:-**There are many versions of spatial steganography, directly change some bits in the image pixel values in hiding data[ 14]. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many detectable distortions. Changes in the value of the LSB are undetectable for human eyes.
2. **Transform Domain Technique:-** This is a more complex way of hiding data in an image [14]. Various techniques and conversion are used on the image to hide data in it. Transform domain embedding can be termed as a domain of implanting techniques for which a number of algorithms have been proposed. The process of implanting data in the frequency domain of a signal is much stronger than implanting principles that operate in the time domain. Most of the powerful steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cutting and image processing. Some techniques of transform domain do not seem dependent on the image format and they may outrun lossless and lossy format conversions.
3. **Distortion Techniques:-** Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the unknown message. The encoder adds a sequence of replaces to the cover image. So, data is described as being saved by signal distortion.
4. **Masking and Filtering:-**These techniques hide information by selecting an image, in the similar way as to paper watermarks[14 ]. These techniques embed the data in the more significant areas than just hiding it into the noise level. The hidden information is more integral to the cover image. The techniques of watermarking can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

### **IV. LITERATURE SURVEY**

- 4.1 **An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography:-** This paper[Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain ] presented in IEEE 2014.In this paper a digital image consists of different pixels. we used color image. As we know, a colored pixel can be represented as a collection of red, green and blue color with appropriate proportions. Color level is represented by a stream of 8 bits in binary notation. Therefore in total, 24 bits are required to denote a pixel. Thus an image is an group of many bytes each representing a single color information deceitful in a pixel. In the proposed technique, a group of three sequential bytes from such an array is used to embed a bit of the entire message.
- 4.2 **A New Approach for LSB Based Image Steganography using Secret Key:-**This paper [S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain] presented in IEEE 2011.This paper introduces a best approach for Least Significant Bit (LSB) based on image steganography that enhances the existing LSB substitution techniques to improve the security level of hidden iriformation.Hidden information is stored into different position of LSB of image depending on the secret key. As a result, it is difficult to withdraw the hidden iriformation knowing the retrieval methods. We have used the Peak Signal-to-Noise Ratio (PSNR) to measure the quality of the stego images. The value of PSNR gives better result because our proposed method changes very small number of bits of the image.
- 4.3 **Metamorphic Cryptography A Paradox between Cryptography and Steganography Using Dynamic Encryption:-**This paper [Thomas Leontin Philjon, Venkateshvara Rao] presented in IEEE 2011 proof security to information being communicated over a network. This paper fuses the two methods and a new technique – Metamorphic Cryptography is born. The message is converted into a cipher image using a key, concealed into another image using Steganography by converting it into an intermediate text and finally transformed once again into an image. The proposed technique thus achieves a high degree of security for information.Portable Network

Graphics format is used to save the images as they consume little space even when the size of the image is drastically increased. This prevents the problem of traffic in the network which arises when the size of the data to be transmitted securely is increased. The technique can be further enhanced by making this method compatible to encrypt audio or video or any other data which has to be transmitted securely.

- 4.4 Highly Randomized Image Steganography using Secret Keys:-**This paper [Sunny Dagar] presented in IEEE 2014. Secret message inside a carrier like image, audio, video. This paper proposes a new approach of image steganography which uses two secret keys to randomize the bit hiding process. Use of two secret keys enhances the security of secret facts. This approach maintains high information hiding capacity like LSB substitution but maintains a much better security level, which is not present in LSB substitution as LSB interchange technique is predictable. As the secure information is highly randomized, so it is hard for attacker to retrieve the secret information from stego image. I used PSNR value to choose the quality of stego image and also compare it with other efficient image steganography techniques.
- 4.5 Data Hiding Using Steganography:-**This paper [Monica Adriana, Emil Ioan Slusanschi, Razvan Dobre] presented in IEEE 2013. The goal of this project was to implement an application that uses the LSB steganography method in order to hide and recover data. The parallelization of the serial version of the algorithm was done using boss-worker threading model. Both data hiding and data recovery can be done in parallel. Neither process depends on the number of threads, and thus any combination of threads can be used. The only variables that must be constant for both processes are the number of bits used from each color component and the size of the chunks in which the input image is divided in order to parallel encode and decode the data.
- 4.6 Securing Data by Using Cryptography with Steganography:-**This paper [Ajit Singh] presented in IJARCSSE 2013. In this paper two layers of security i.e. cryptography and steganography are used which makes it difficult to detect the presence of hidden message. Cryptography Blowfish algorithm is used which is much better than AES and DES. In order to fragment blowfish algorithm he has to spend a lot of time and effort for trying several attacks and getting the actual message. Although both of these techniques are easy to implement but their combination will provide much efficient and reliable security.

Survey paper	Methods and Algorithm	Performance
LSB Image steganography using status bit along with AES cryptography	Filtering Algorithm using AES cryptography and Image steganography	PSNR value of proposed technique is better.
Image steganography using secret key	LSB method and secret key 1D array of bit stream	Lower distortion and good image Quality
A Paradox between Cryptography and Steganography Using Dynamic Encryption	Paradox cryptography and steganography	Consume little space and even when the size of image drastically increased
Highly Randomized Image Steganography using Secret Keys	LSB steganography and cryptography	High data hiding capacity
Data Hiding Using Steganography	Parallelization of the serial version of the Algorithm	Noise detection and less time consuming
Securing Data by Using Cryptography with Steganography.	Blowfish Algorithm and LSB steganography	More efficient and reliable security

## V. PROPOSED WORK

In this paper we use MATLAB to implement image compressed steganography and DES cryptography. Using these methods of steganography and cryptography PSNR value is increased than other methods and security level of information is also increased.

## VI. CONCLUSION

In this paper, we have reviewed the new field of steganography and cryptography. In future there are several directions with this method to improve the capacity and PSNR value. The combination of both techniques provided secret message can be secured by two security layers.

## REFERENCES

- [1] Md. Rashedul Islam, Ayasha Siddiqua, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" 3rd International Conference On Informatics, Electronics & Vision 2014.
- [2] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key" Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011) 22-24 December, 2011.
- [3] Thomas Leontin Philjon, Venkateshvara Rao "Metamorphic Cryptography A Paradox between Cryptography and Steganography Using Dynamic Encryption" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.

- [4] Sunny Dagar “Highly Randomized Image Steganography using Secret Keys” IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014.
- [5] Monica Adriana, Emil Ioan Slusanschi, Razvan Dobre“Data Hiding Using Steganography” 2013 IEEE 12th International Symposium on Parallel and Distributed Computing.
- [6] Ajit Singh “Securing Data by Using Cryptography with Steganography” International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013.
- [7] S. Rubab and M. Younus, “Improved Image Steganography Technique for Colored Images using Wavelet Transform”,International Journal of Computer Applications, Volume 39–No.14, pp. 29-32, 2012.
- [8] Clair, Bryan. “Steganography: How to Send a Secret Message.” 8 Nov.2001.
- [9] Jassim Mohmmmed Ahmed and Zulkarnain Md Ali "Information Hiding using LSB technique" IJCSNS International 18 Journal of Computer Science and Network Security, VOL.II No.4, April 2011.
- [10] Jose, J.A.; Titus, G., "Data hiding using motion histogram," Computer Communication and Informatics (ICCCI), 2013 International Conference on , vol., no., pp.1,4, 4-6 Jan. 2013.
- [11] A Castiglione, U Fiore, F. Palmieri, "E-mail-based Covert Channels for Asynchronous Message Steganography", 5th IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 503-508,2011.
- [12] Deepali, “Steganography with Data Integrity”, International Journal of Computational Engineering Research, Vol. 2, Issue No. 7, 2012 .
- [13] Anil Kumar , Rohini Sharma “A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3,july 2013.
- [14] Mehdi Hussain and Mureed Hussain “ A Survey of Image Steganography Techniques” International Journal of Advanced Science and Technology Vol. 54, May, 2013.